

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
MISSOULA DIVISION**

IN THE MATTER OF THE SEARCH OF
CONTENT OF AND RECORDS RELATING
TO ACCOUNTS
MEYONEA0707@GMAIL.COM,
MEYONEER@GMAIL.COM AND
PIMAZON@GMAIL.COM THAT ARE
STORED AT PREMISES CONTROLLED
BY GOOGLE, INC.

Case No. MT-18-10-M-JCL

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Shiloh A. Allen, being first duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, Inc. (Google), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), and to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since April 13, 2008. Currently, I am assigned to the Cyber Crime Squad of the Salt Lake

City, Utah Field Office. My experience as an FBI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of fraud and intrusion. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment as well as interview and interrogation of subjects of cyber crimes.

3. This affidavit is intended to show merely that there is probable cause sufficient for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4), 1343, 2511(1)(a) and 2511(1)(d) have been committed by a person or group using the names Solomon A. Nwachukwu and Godspower C. Nwachukwu, who registered and used email accounts meyonea0707@gmail.com, meyoneer@gmail.com and pimazon@gmail.com. There is also probable cause to search the above accounts, further described in Attachment A, for the items specified in Attachment B, which constitute evidence, instrumentalities, or fruits of the foregoing violations.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A),

and 2703 (c)(1)(A). Specifically, the United States District Court for the District of Montana is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND CONCERNING EMAIL

6. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account registration information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

7. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, and other files, on servers maintained, owned, leased or otherwise controlled by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails in the account, and attachments to emails, including pictures and files.

8. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers, and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

9. In my experience, many email providers, including Google, Microsoft Corporation (Microsoft), Yahoo! Inc. (Yahoo), and AOL, Inc. (AOL) encourage subscribers to provide an additional email address, sometimes referred to as a backup account, recovery account, alternate email, or secondary address. The purpose of this backup account is to provide a means whereby the subscriber can recover access to their email account in the event that they forget or lose their password. The email provider will use the additional email address as an alternate channel of communication to transmit password recovery information to the subscriber. Because of this, the additional email address provided by a subscriber must be one they control and have access to. Therefore, in my experience, additional email address information may constitute evidence of the crimes under investigation because such information can be used to identify additional accounts used by a subject or subjects, which may contain information about the crimes under investigation, as well as information that can be used to identify a subject or subjects.

10. In my training and experience, although the personal identifying information requested by an email provider from a subscriber is not validated and can be easily falsified, the

contents of email communications can contain the subscriber's true information, such as name, address, telephone number, and other email addresses and communications facilities used by a subscriber. Further, the contents of email messages can contain identifying information of other unknown subjects and additional victims. The contents of emails can also hold written conversations between the subscriber and his/her contacts discussing activities related to the crimes under investigation. Therefore, in my training and experience, the information found in the contents of email messages may constitute evidence of the crimes under investigation because such information can be used to identify subjects, accomplices, additional victims, and further details about the crimes under investigation, such as motives and methods.

11. In my training and experience, email providers such as Google typically retain certain transactional information about the creation and use of each account on their systems, including associative information between accounts and the devices that access them. This information can include the date on which the account was created, the length of service, records of login (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

12. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

BACKGROUND CONCERNING MONEY MULES

13. In my training and experience, I know that many schemes involving the fraudulent transfer of money use a technique called "money mules" to channel and launder the money from the victim to the perpetrator of the fraud. Money mules people who receive fraudulent money transfers into their personal or business accounts and transfer the money to yet another destination by various means including, but not limited to, Western Union, MoneyGram, ACH or SWIFT wire transfer, and crypto-currency networks such as Bitcoin.

14. Sometimes, money mules are knowing members of a money laundering network and are witting participants in the fraud scheme. Often times, however, a money mule does not realize they are participating in a fraud scheme. Perpetrators of the fraud scheme often recruit money mules under false pretexts, such as posing as a legitimate employer offering work-from-home opportunities or claiming to be a venture capitalist seeking investment opportunities and business partnerships. A money mule recruited under such pretexts then receives and sends

money at the instruction of the perpetrators, believing they are engaging in legitimate financial activities.

15. The money mule's handler is sometimes directly involved in the fraud scheme. Alternatively, the money mule's handler may be a specialist who focuses exclusively on recruiting and managing a network of money mules, and provides money laundering services for hire to various groups operating distinct and unrelated fraud schemes.

FACTS ESTABLISHING PROBABLE CAUSE

16. Bruce Robert Harbour of 9156 River Road, Bozeman, Montana 59718 maintains a money market account under the name of his holding company, Hell Creek Holdings, LLC with First Interstate Bank, 2023 Burke Street, Bozeman, Montana 59718. Mr. Harbour, who was out of the country on extended travel for a period of time including March 30, 2016 through June 23, 2016, employed the services of Deb Dechert, 3016 Bridger Canyon Road, Bozeman, Montana 59715, as his book keeper to maintain his accounts and other financial and legal affairs in his absence. Mr. Harbour and Ms. Dechert communicated primarily by email, due to time zone differences that made telephone communication difficult. Mr. Harbour used email account bharbour88@live.com and Ms. Dechert used email account debdechert@hotmail.com.

17. Between March 30, 2016 and June 23, 2016, Ms. Dechert received several emails from email account bharbour88@live.com instructing her to wire money from Mr. Harbour's money market account to various beneficiary accounts, later identified as money mules, across the United States. After the last wire transfer was made on June 23, 2016, Mr. Harbour's money market account was almost entirely depleted. Lack of funds for a legitimate transaction Mr.

Harbour sought to complete prompted Mr. Harbour and Ms. Dechert to review all of the account activity and their communications over the past several months.

18. Upon reviewing the history of emails containing wire transfer requests that Ms. Dechert had received, Mr. Harbour and Ms. Dechert identified 10 wire transfer requests that Mr. Harbour had no knowledge of. All 10 wire transfer requests originated from Mr. Harbour's legitimate email account, bharbour88@live.com, even though Mr. Harbour did not send them. This indicates that a heretofore unidentified person or persons obtained unauthorized access to Mr. Harbour's email account and used it to send the wire transfer requests to Ms. Dechert. The total loss to Mr. Harbour from these fraudulent wire transfers was approximately \$696,000 USD.

19. The investigation identified several email accounts associated with the person or group responsible for above described computer intrusion and fraud, as well as the handling and coordination of the money laundering through the various money mules. Among these were email accounts were soloalexfin@gmail.com, alexlukacher@outlook.com, and soloheat2002@yahoo.com. Subpoenas and search warrants were served on Google, Microsoft, and Yahoo targeting theses accounts.

20. The return information included email message contents, subscriber records, and IP login history for each account, which contained facts establishing that soloalexfin@gmail.com, alexlukacher@outlook.com, and soloheat2002@yahoo.com are likely owned and controlled by the same person or group of collaborators. A subpoena was served on Microsoft seeking IP address login history for Mr. Harbour's email account bharbour88@live.com, which contained records indicating that the person or group using email

accounts soloalexfin@gmail.com, alexlukacher@outlook.com, and soloheat2002@yahoo.com was also responsible for the unauthorized access to bharbour88@live.com.

21. Search warrant returns for email accounts soloalexfin@gmail.com, alexlukacher@outlook.com and soloheat2002@yahoo.com also contained information which indicated the possible names or aliases used by the person or group using these accounts, as well as additional email accounts.

SOLOMON A. NWACHUKWU

22. Account registration information for soloheat2002@yahoo.com contained the name Mr. Solomon Nwachukwu. Emails from Nigerian financial institutions Guaranty Trust Bank (GTBank) and Diamond Bank, sent directly to email account soloheat2002@yahoo.com, contained financial statements that were addressed to Solomon Azunna Nwachukwu (Solomon A. Nwachukwu). This demonstrates that Solomon A. Nwachukwu is likely the name of the person who owns and controls email account soloheat2002@yahoo.com.

23. Google subscriber information for account soloalexfin@gmail.com listed soloheat2002@yahoo.com as its Recovery email account, indicating that soloalexfin@gmail.com is also owned and controlled by Solomon A. Nwachukwu. Analysis results of IP address logon records for email accounts soloheat2002@yahoo.com, soloalexfin@gmail.com and alexlukacher@outlook.com showed multiple instances where one IP address was used to log in to all three accounts within a short time span, further establishing reason to believe that soloheat2002@yahoo.com and soloalexfin@gmail.com are owned and controlled by the same person, and indicating that alexlukacher@outlook.com is also owned and controlled by this

person; presumably, Solomon A. Nwachukwu. Cross analysis of these IP address logon records with IP address logon records for victim account bharbour88@live.com indicated that Solomon A. Nwachukwu is also the person who obtained unauthorized access to bharbour88@live.com.

GODSPower C. NWACHUKWU

24. Multiple emails discovered in email accounts soloheat2002@yahoo.com and soloalexfin@gmail.com contained airline ticket information for passengers Solomon A. Nwachukwu and Chinecherem Ukaegbu. The account that forwarded the airline ticket information to soloheat2002@yahoo.com and soloalexfin@gmail.com was meyonea0707@gmail.com, contact name "Godspower C. Nwachukwu".

25. An open source, online search for the name Godspower C. Nwachukwu revealed Facebook account facebook.com/cligence with the display name Godspower C. Nwachukwu. An open source, online search for the name Chinecherem Ukaegbu revealed Facebook account facebook.com/chinecherem.ukaegbu1 with the display name Chinecherem Ukaegbu. Ms. Ukaegbu's Facebook Friends list included Godspower C. Nwachukwu, account facebook.com/cligence.

26. Godspower C. Nwachukwu's email address was listed on his Facebook page as meyonea0707@gmail.com. Godspower C. Nwachukwu's Facebook page also listed him as the Director of Pimazz, with a link to the Pimazz Facebook page. Pimazz appears to be an online retail company. The Pimazz Facebook page listed a contact email address of meyoneer@gmail.com. Godspower C. Nwachukwu's Facebook page also listed his website as www.pimazon.com. A Federal Grand Jury subpoena served on Facebook for subscriber records

pertaining to Godspower C. Nwachukwu's Facebook page revealed that Godspower C. Nwachukwu registered a PayPal account with Facebook under the email account pimazon@gmail.com. Domain Whois records for www.pimazon.com showed the following registrant information:

www.pimazon.com:

Registrant Name: Cligence

Registrant Organization: Pimazon

Registrant Street: 669

Registrant City: Jos

Registrant State/Province: Plateau

Registrant Postal Code: 234

Registrant Country: NG

Registrant Phone: +234.7030197973

Registrant Email: meyonea0707@gmail.com

27. A reverse whois lookup of meyonea0707@gmail.com showed that the domains www.pimaxchange.com and www.pimaxchange.net were also registered with email address meyonea0707@gmail.com. Additional registrant information for domains www.pimaxchange.com and www.pimaxchange.net differed from that of www.pimazon.com as can be observed below:

www.pimaxchange.com:

Registrant Name: Godspower Nwachukwu

Registrant Organization: Pimazon

Registrant Street: Zone 5 Lugbe HSE 31 ABJ

Registrant City: FCT

Registrant State/Province: Abia

Registrant Postal Code: 234

Registrant Country: NG

Registrant Phone: +1.7030197973

Registrant Email: meyonea0707@gmail.com

www.pimaxchange.net:

Registrant Name: Godspower Nwachukwu

Registrant Organization: Meyoneer Limited

Registrant Street: Zone 5 Lugbe HSE 31 ABJ

Registrant City: FCT

Registrant State/Province: Abuja

Registrant Postal Code: 500001

Registrant Country: NG

Registrant Phone: +234.7030197973

Registrant Email: meyonea0707@gmail.com

28. (U) In addition to the examples above where email account meyonea0707@gmail.com, attributed to Godspower C. Nwachukwu, communicated with email accounts attributed to Solomon A. Nwachukwu, there were multiple other emails discovered in email accounts soloheat2002@yahoo.com, soloalexfin@gmail.com, and alexlukacher@outlook.com from email account meyonea0707@gmail.com involving collaboration on various fraud schemes and movement of funds. This indicates that Solomon A. Nwachukwu and Godspower C. Nwachukwu are either aliases for the same person, or they are the names of two distinct people who are accomplices and collaborators.

29. Email accounts pimazon@gmail.com and meyoneer@gmail.com appear to be openly affiliated with endeavors undertaken by Godspower C. Nwachukwu to present or establish an online storefront or business at the various domains www.pimazon.com, www.pimaxchange.com and www.pimaxchange.net. As such, there is reason to believe that Godspower C. Nwachukwu's communications using email accounts pimazon@gmail.com and meyoneer@gmail.com may reveal more true or accurate information necessary to locate and fully identify Godspower C. Nwachukwu, because these communications are less likely to be made using precautions to hide Godspower C. Nwachukwu's true location or identity.

CONCLUSION

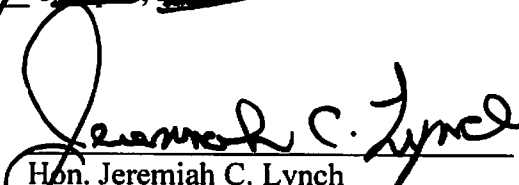
30. Based on the forgoing, I conclude there is probable cause to believe that Godspower C. Nwachukwu and Solomon A. Nwachukwu are either aliases for the same person, or they are the names of two distinct individuals who are members of the same collaborative group, and this person or group is responsible for the criminal activity described above. Further,

there is probable cause to believe that this person or group, who is already known to use and control email accounts alexlukacher@outlook.com, soloheat2002@yahoo.com and soloalexfin@gmail.com, also uses and controls email accounts meyonea0707@gmail.com, meyoneer@gmail.com and pimazon@gmail.com. I, therefore, conclude there is probable cause to believe that the email accounts meyonea0707@gmail.com, meyoneer@gmail.com and pimazon@gmail.com, which are stored at premises controlled by Google, contain information which constitutes evidence of violations of 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4), 1343, 2511(1)(a) and 2511(1)(d), as described above and under attachment B.

Respectfully submitted,

Shiloh A. Allen
Special Agent
Federal Bureau of Investigation
Bozeman, Montana

Subscribed and sworn before me this 2/27/18 at Bozeman, Montana


Hon. Jeremiah C. Lynch
United States Magistrate Judge